

# Office Action Summary

**Application No.**

10/767,004

**Applicant(s)**

CUI ET AL.

**Examiner**

JEFFREY D. POPHAM

**Art Unit**

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 20 February 2008.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-45 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-45 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 28 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO/S508)  
Paper No(s)/Mail Date \_\_\_\_\_  
4) ☒ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: 20080524  
5) ☐ Notice of Informal Patent Application  
6) ☐ Other: \_\_\_\_\_

***Remarks***

Claims 1-45 are pending.

Art regarding the points discussed during the interview for possible amendment has been cited in the conclusions section of this office action.

***Response to Arguments***

1. Applicant's arguments filed 2/20/2008 have been fully considered but they are not persuasive.

Applicant argues that the claimed invention determines levels of trust not based on performing accesses or other operations. There does not appear to be anything in the claims that limits determining of levels of trust to not being based on accessing data. Claim 18 describes the client "sending a request to the server for content, wherein the request includes an identifier associated with a user agent", which appears to be the opposite of what Applicant is arguing, since the request that seems to trigger the trust level determination is an explicit request to access content.

Applicant argues that Jamtgaard does not teach testing for capabilities of mobile devices (being enabled to accept a cookie or interact with a URL). As discussed in the interview, the claims do not actually recite checking or testing the capabilities of the device, only that, if the mobile device is enabled to accept a cookie, determining at least a second level of trust; and, if the mobile device is enabled to interact with a URL, determining at least a third level of trust. However, column 8, lines 31-34 of Jamtgaard shows determination of capabilities of a client, in that "The appliance connection handler

44 examines header information from the requesting data in order to determine a target device 15, protocol and browser configuration.”

Applicant argues that Jamtgaard does not teach determining a level of trust based on the capability of being enabled to accept cookies. The specification and claims of the current application do not make clear what the purpose of the trust level is, other than that it is to determine a signature for the mobile device. While Jamtgaard may not explicitly state trust levels within the capability-based translation system, the functionality appears to provide a corresponding level determination. Without knowledge of what, precisely, a level of trust entails or is used for, it is difficult to determine exactly what the level of trust is. Jamtgaard clearly teaches determining the functionality of capabilities of a device and using such determination to translate data into a form that the client can process. The translation server of Jamtgaard will determine whether or not a particular device can support cookies or javascript, for example. If the device cannot support them, the translation server will provide javascript and/or cookie proxy engines, so that the web site being communicated with thinks that the client has such functionality. The translation server will then provide such processed/translated data to the client, the data being formatted specifically for the client's capabilities. As can be seen in column 14, lines 17-18 of Jamtgaard, for example, “the class attribute allows different levels of content to be presented to different classes of devices.” The devices have a classification based on functionality/capabilities, which is used by Jamtgaard in order to properly translate, convert, and proxy data and functionality for the specific classes of devices.

Applicant argues that Jamtgaard does not make a determination of whether or not the mobile device is capable of interacting with a URL. As discussed in the interview, this limitation was taken as the default level of trust that any device is allowed access to (see claim 8). It turns out that this may not be the case, and that the claims may have been worded badly, but that is the interpretation that was taken and is currently held regarding the URL. All devices connecting to the system of Jamtgaard have the ability to interact with URLs and, therefore, all device are assigned at least a third level of trust.

Applicant argues that "Aura appears to seek to limit access to content based on authentication; Jammtgaard provides a virtual browser that is not on the mobile device but is directed towards allowing access to different content. Thus, any combination of Jammtgaard would clearly change the principle operation of Aura." One will note that Jamtgaard is not concerned with providing data to the client for which the client should not have access, but is concerned with providing data in such a manner that the client can process and use such data, even when the client does not have the appropriate functionality to do so by itself, by translating and converting the data into a format appropriate for the specific client device's capabilities. Aura is entirely concerned with authentication and authorization, providing access based on levels of trust. Within the combination, one will clearly see that devices are only allowed access to data for which they are authorized, and that this data may be translated into a form readily usable by the client, such that clients with lesser capabilities can still use all data for which they have access.

Regarding claim 7, Applicant argues that Laraki "does not even teach at paragraphs 33-37 and 46-52 a subscription identifier or a gateway group identifier at all!". As noted by Applicant, a gateway may be configured to generate a subscription identifier based, in part, on the MIN number, and other information provided by mobile device that may uniquely identify the mobile device. Paragraphs 33-37 of Laraki describe a proxy determining, replacing, and/or adding an identifier regarding a subscription, to a request. Paragraphs 46-52 further this by giving example embodiments. One of these embodiments uses an alias based upon the UID of the device and the service ID of the requested subscription service. Paragraph 53 describes examples of a UID, one of them being a 10 digit telephone number of the mobile device (MIN). Paragraphs 56-72 describe how to generate an alias (or subnym). This subnym may be generated using the UID (paragraph 59), as well as other information. As it has been shown that Laraki's proxy/gateway can generate the subscription identifier (alias/subnym) by use of the device's MIN (UID shown in paragraph 53), it should be clear that Laraki teaches such a subscription identifier. For clarity, the rejection now cites paragraphs 53-72 for explicit showing of the generation of the alias referred to in the previously cited sections.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-4, 8-12, 14, 15, 26-30, 32, 35-38, and 40-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura (U.S. Patent 6,947,725) in view of Jamtgaard (U.S. Patent 6,430,624).

Regarding Claim 1,

Aura discloses a method of managing a communication with a mobile device over a network, comprising:

Receiving a request from the mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

Automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23) and based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

If the mobile device is enabled to access the Internet, then determining at least a third level of trust associated with the mobile device (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19); and

Determining at least one device signature for the mobile device based on the at least one level of trust from the plurality of different levels of trust, and independent of user authentication (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27);

But may not explicitly disclose if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device and if the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device.

Jamtgaard, however, discloses if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and determining that the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device (Column 5, lines 27-53; Column 8, line 4 to Column 9, line 22; and Column 14, lines 4-20). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability determination and translation system of Jamtgaard into the mobile authentication system of Aura in order to allow the system to determine device capabilities and to translate data accordingly so that the device can receive properly formatted data that the device can understand, while allowing capabilities that the device

does not have to be run by a proxy system, thereby providing use of the capabilities even when the device itself cannot perform such capabilities.

Regarding Claim 2,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and determining the at least one level of trust based, in part, on the associated information and the gateway information (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 3,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses that the associated information comprises at least one of a device identifier, user agent information, and an indication that the mobile device is enabled to accept a cookie (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 4,

Aura as modified by Jamtgaard discloses the method of claim 3, in addition, Aura discloses that the associated information further comprises at least one of a gateway group identifier and a subscription identifier (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).



Regarding Claim 8,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses determining a default level of trust as the third level of trust (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19).

Regarding Claim 9,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses that the mobile device identifier is at least one of a MIN, ESN, application serial number, or a mobile telephone number (Column 13, line 64 to Column 15, line 6).

Regarding Claim 10,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 11,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises if the second level of trust is determined, determining a

second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 12,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises if the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 14,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses that determining at least one device signature further comprises employing a hash function selected from at least one of a message digest, SHA, DES, 3DES, HAVAL, RIPEMD, and Tiger hash function (Column 4, lines 58-62).

Regarding Claim 15,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses expiring the at least one device signature based,

in part, on a predetermined period of time associated with each of the at least one device signature (Column 9, line 43 to Column 10, line 27).

Regarding Claim 26,

Aura discloses a server for managing a communication with a mobile device over a network comprising:

A transceiver for receiving a request from the mobile device and for sending at least one device signature to the mobile device (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

A transcoder that is configured to perform actions including:

Receiving the request from the mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

Automatically determining at least one level of trust from a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23) and further based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

If the mobile device is enabled to access the Internet, then determining at least a third level of trust associated with the mobile device

(Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19); and

Determining the at least one device signature for the mobile device based on the at least one level of trust of the plurality of different trust levels, wherein the at least one device signature is independent of user authentication (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27);

But may not explicitly disclose if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device and if the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device.

Jamtgaard, however, discloses if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and determining that the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device (Column 5, lines 27-53; Column 8, line 4 to Column 9, line 22; and Column 14, lines 4-20). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability determination and translation system of Jamtgaard into the mobile authentication system of Aura in order to allow the system to determine device capabilities and to translate

data accordingly so that the device can receive properly formatted data that the device can understand, while allowing capabilities that the device does not have to be run by a proxy system, thereby providing use of the capabilities even when the device itself cannot perform such capabilities.

Regarding Claim 27,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses that the transcoder is configured to perform actions comprising receiving gateway information, wherein the gateway information is associated with a carrier gateway for the mobile device; and determining the at least one level of trust based, in part, on the associated information and the gateway information (Column 4, lines 32-65; Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 28,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses that determining the at least one device signature comprises if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 29,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses that determining the at least one device signature further comprises if the second level of trust is determined, determining a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 30,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses that determining the at least one device signature further comprises if the third level of trust is determined, determining a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 32,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses that determining the at least one level of trust further comprises determining the second level of trust based at least one of a gateway identifier, and a user agent (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 35,

Aura discloses a system for managing a communication with a mobile device over a network comprising:

The mobile device configured to provide information associated with the mobile device (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

A server, coupled to a carrier gateway, that is configured to receive the associated information and to perform actions (Column 4, lines 32-65; Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23), including:

Automatically determining at least two different levels of trust from a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23), wherein the at least two different levels of trust are based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and

Determining another level of trust associated with the mobile device (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

Initially determining at least two different device signatures for the mobile device each of the two device signatures being based on a different one of the at least two different levels of trust, wherein the at least two device signatures are each determined independent of user authentication (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

But may not explicitly disclose determining if the mobile device is enabled with a defined operational capability.

Jamtgaard, however, discloses determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device (Column 5, lines 27-53; Column 8, line 4 to Column 9, line 22; and Column 14, lines 4-20). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability determination and translation system of Jamtgaard into the mobile authentication system of Aura in order to allow the system to determine device capabilities and to translate data accordingly so that the device can receive properly formatted data that the device can understand, while allowing capabilities that the device does not have to be run by a proxy system, thereby providing use of the capabilities even when the device itself cannot perform such capabilities.

Regarding Claim 36,



Aura as modified by Jamtgaard discloses the system of claim 35, in addition, Aura discloses that determining the at least two device signatures further comprises determining a tier 1 device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 37,

Aura as modified by Jamtgaard discloses the system of claim 35, in addition, Aura discloses that determining the at least two device signatures further comprises determining a tier 2 device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 38,

Aura as modified by Jamtgaard discloses the system of claim 35, in addition, Aura discloses that determining the at least two device signatures further comprises determining a tier 3 device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 40,

Aura as modified by Jamtgaard discloses the system of claim 35, in addition, Aura discloses a carrier gateway, coupled to the mobile device, that is configured to receive the associated information, and provide the associated information and gateway information related to the carrier gateway (Column 4, lines 32-65; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 41,

Aura discloses a computer readable storage medium for communicating with a mobile device, the computer readable storage medium having computer executable instructions stored thereon that when installed into a computing device enable the computing device to perform actions, comprising:

Receiving a request from the mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

Sending at least one device signature to the mobile device based on at least one level of trust determined from a plurality of different levels of trust that is determined, in part, using the associated information (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27), wherein the at least one level of trust is based on:

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated

with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and

Determining another level of trust associated with the mobile device, and wherein the at least one device signature is determined independent of user authentication (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

But may not explicitly disclose determining if the mobile device is enabled with a defined operational capability.

Jamtgaard, however, discloses determining if the mobile device is enabled with a defined operational capability and if the mobile device is so enabled, then determining another level of trust associated with the mobile device (Column 5, lines 27-53; Column 8, line 4 to Column 9, line 22; and Column 14, lines 4-20). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability determination and translation system of Jamtgaard into the mobile authentication system of Aura in order to allow the system to determine device capabilities and to translate data accordingly so that the device can receive properly formatted data that the device can understand, while allowing capabilities that the device does not have to be run by a proxy system, thereby providing use of the capabilities even when the device itself cannot perform such capabilities.

Regarding Claim 42,

Aura as modified by Jamtgaard discloses the computer readable storage medium of claim 41, in addition, Aura discloses that determining the at least one device signature further comprises if the first level of trust is determined, determining a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 43,

Aura as modified by Jamtgaard discloses the computer readable storage medium of claim 41, in addition, Aura discloses that determining the at least one device signature further comprises if the other level of trust is determined, determining another device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, a user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 44,

Aura as modified by Jamtgaard discloses the computer readable storage medium of claim 41, in addition, Aura discloses that determining the at least one device signature further comprises if the other level of trust is determined, determining another device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a

time (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6)

Regarding Claim 45,

Aura discloses an apparatus for communicating with a mobile device comprising:

A means for receiving a request from a mobile device, wherein the request includes associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23);

A means for automatically determining a plurality of different levels of trust based, in part, on the associated information (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); and

A means for determining a plurality of different device signatures for the mobile device based, in part, on the determined plurality of different levels of trust, and independent of user authentication (Column 7, line 42 to Column 8, line 23; and Column 9, line 43 to Column 10, line 27);

But may not explicitly disclose that the associated information indicates a capability of the mobile device and that at least one of the different levels of trust is based on an operational capability of the mobile device.

Jamtegaard, however, discloses that the associated information indicates a capability of the mobile device and that at least one of the different levels of trust is based on an operational capability of the mobile

device (Column 5, lines 27-53; Column 8, line 4 to Column 9, line 22; and Column 14, lines 4-20). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability determination and translation system of Jamtgaard into the mobile authentication system of Aura in order to allow the system to determine device capabilities and to translate data accordingly so that the device can receive properly formatted data that the device can understand, while allowing capabilities that the device does not have to be run by a proxy system, thereby providing use of the capabilities even when the device itself cannot perform such capabilities.

3. Claims 5, 18, 20-22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Jamtgaard, further in view of Wilf (U.S. Patent 6,496,824).

Regarding Claim 5,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses automatically determining a second device signature based on a second level of trust, wherein the second device signature comprises a hash of at least a gateway group identifier (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); but does not explicitly disclose that the signature hash also comprises

a cookie and a user agent identifier obtainable from the associated information.

Wilf, however, discloses that the signature hash also comprises at least a cookie and a user agent identifier obtainable from the associated information (Column 4, lines 5-35). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management techniques of Wilf into the mobile authentication system of Aura in order to provide a stronger signature, based upon more client and/or gateway specific information, thus increasing security of the signature and making it harder to forge.

Regarding Claim 18,

Aura discloses a client adapted for a mobile device to communicate with a server over a network, the client being configured to perform actions comprising:

Sending a request to the server for content, wherein the request includes an identifier associated with the device (Column 5, line 58 to Column 6, line 13; Column 7, line 42 to Column 8, line 23; and Column 13, line 64 to Column 15, line 6);

Receiving at least one device signature associated with the mobile device, wherein the at least one device signature is based on at least one level of trust determined from a plurality of different trust levels, and is independent of user authentication (Column 5, line 58 to Column 6, line

13; and Column 7, line 42 to Column 8, line 23), the at least one level of trust being determined based on:

Determining at least a default level of trust (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19);

If a trusted mobile device identifier associated with the mobile device is received, then determining at least a first level of trust associated with the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6); and

If the mobile device is enabled to access the Internet, then determining at least a third level of trust associated with the mobile device (Column 3, line 31 to Column 4, line 11; Column 7, line 42 to Column 8, line 23; and Column 9, lines 4-19); and

But may not explicitly disclose if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device and if the mobile device is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device; or that the identifier associated with the device comprises an identifier associated with a user agent.

Jamtgaard, however, discloses if the mobile device is enabled to accept a cookie, then determining at least a second level of trust associated with the mobile device; and determining that the mobile device



is enabled to interact with a URL, then determining at least a third level of trust associated with the mobile device (Column 5, lines 27-53; Column 8, line 4 to Column 9, line 22; and Column 14, lines 4-20). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability determination and translation system of Jamtgaard into the mobile authentication system of Aura in order to allow the system to determine device capabilities and to translate data accordingly so that the device can receive properly formatted data that the device can understand, while allowing capabilities that the device does not have to be run by a proxy system, thereby providing use of the capabilities even when the device itself cannot perform such capabilities.

Wilf, however, discloses that the identifier associated with the device comprises an identifier associated with a user agent (Column 4, lines 5-35). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management techniques of Wilf into the mobile authentication system of Aura in order to provide a stronger signature, based upon more client and/or gateway specific information, thus increasing security of the signature and making it harder to forge.

Regarding Claim 20,

Aura as modified by Jamtgaard and Wilf discloses the client of claim 18, in addition, Aura discloses that receiving the at least one device

signature further comprises if the at least one device signature is based on the first level of trust, receiving a first tier device signature based, in part, on a hash of at least one of a subscription identifier, a gateway group identifier, the user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 21,

Aura as modified by Jamtgaard and Wilf discloses the client of claim 18, in addition, Aura discloses that receiving the at least one device signature further comprises if the at least one device signature is based on the second level of trust, receiving a second tier device signature based, in part, on a hash of at least one of a cookie, a gateway group identifier, the user agent identifier, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 22,

Aura as modified by Jamtgaard and Wilf discloses the client of claim 18, in addition, Aura discloses that receiving the at least one device signature further comprises if the at least one device signature is based on the third level of trust, receiving a third tier device signature based, in part, on a hash of at least one of a gateway group identifier, a user agent identifier, a server identifier, a process identifier, a random number, and a time stamp (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6).

Regarding Claim 24,

Aura as modified by Jamtgaard and Wilf discloses the client of claim 18, in addition, Jamtgaard discloses that receiving the at least one device signature further comprises, if the request indicates the mobile device is enabled to accept a cookie, associating the cookie with the at least one device signature (Column 5, lines 27-53; and Column 8, line 4 to Column 9, line 22); and Wilf discloses associating the cookie with the at least one device signature (Column 4, lines 5-35).

4. Claims 6, 7, 16, 17, 31, 33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Jamtgaard, further in view of Laraki (U.S. Patent Application Publication 2003/0233329).

Regarding Claim 6,

Aura as modified by Jamtgaard does not explicitly disclose that the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a MIN, ESN, and application serial number.

Laraki, however, discloses that the associated information further comprises a subscription identifier associated with the mobile device that is based on at least one of a MIN, ESN, and application serial number (Paragraph 53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile

subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 7,

Aura as modified by Jamtgaard discloses the method of claim 1, in addition, Aura discloses determining the level of trust of the mobile device identifier and trusting the mobile device if the identifier is so trusted (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

But does not explicitly disclose determining a level of trust of a carrier associated with the mobile device based on at least one of a received subscription identifier and a gateway group identifier, trusting the mobile device identifier based on such carrier trust, and inhibiting the determination of a level of trust associated with the device if the mobile device identifier is not trusted in this manner.

Laraki, however, discloses determining a level of trust of a carrier associated with the mobile device based on at least one of a received subscription identifier and a gateway group identifier, trusting the mobile device identifier based on such carrier trust, and inhibiting the

determination of a level of trust associated with the device if the mobile device identifier is not trusted in this manner (Paragraphs 33-37 and 46-72). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 16,

Aura as modified by Jamtgaard does not explicitly disclose if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature.

Laraki, however, discloses if the at least one device signature has expired, determining if the expired device signature is to be rolled over, and if the expired device signature is to be rolled over, extending a validity period associated with the expired device signature (Paragraphs 45 and 66). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription

services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 17,

Aura as modified by Jamtgaard and Laraki discloses the method of claim 16, in addition, Laraki discloses that determining if the expired device signature is to be rolled over further comprises evaluating at least one of a condition, event, change in an identifier indicating a grouping of the gateway, and a time (Paragraphs 45 and 66).

Regarding Claim 31,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses that determining the at least one level of trust further comprises determining the first level of trust based at least one of a gateway group identifier, a subscription identifier, a user agent, and a security level associated with the request from the mobile device (Column 9, line 43 to Column 10, line 27; and Column 13, line 64 to Column 15, line 6);

But may not explicitly disclose using such information to determine if the mobile device identifier is trusted.

Laraki, however, discloses using such information to determine if the mobile device identifier is trusted (Paragraphs 33-37 and 46-72). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 33,

Aura as modified by Jamtgaard may not explicitly disclose determining that the mobile device identifier is trusted if a carrier gateway associated with the mobile device is trusted.

Laraki, however, discloses determining that the mobile device identifier is trusted if a carrier gateway associated with the mobile device is trusted (Paragraphs 33-37 and 46-72). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for

content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 34,

Aura as modified by Jamtgaard discloses the server of claim 26, in addition, Aura discloses determining if at least one device signature has expired (Column 13, line 64 to Column 15, line 6); but does not explicitly disclose extending a validity period associated with the expired device signature is the expired device signature is to be rolled over.

Laraki, however, discloses determining if at least one device signature has expired and extending a validity period associated with the expired device signature is the expired device signature is to be rolled over (Paragraphs 45 and 66). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.



5. Claims 13 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Jamtgaard, further in view of Kindberg (U.S. Patent Application Publication 2003/0061515).

Regarding Claim 13,

Aura as modified by Jamtgaard does not explicitly disclose including a device signature in a munged URL.

Kindberg, however, discloses including a device signature in a munged URL (Paragraphs 39 and 43-50). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability-enabled URL of Kindberg into the mobile authentication system of Aura as modified by Jamtgaard in order to provide a simple mechanism by which a client can prove authorized access to resources via use of a modified URL including a signature corresponding to a particular capability.

Regarding Claim 39,

Aura as modified by Jamtgaard does not explicitly disclose providing a signature to the mobile device through a munged URL.

Kindberg, however, discloses providing a signature to the mobile device through a munged URL (Paragraphs 39 and 43-50). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability-enabled URL of Kindberg into the mobile authentication system of Aura as modified by Jamtgaard in order to

provide a simple mechanism by which a client can prove authorized access to resources via use of a modified URL including a signature corresponding to a particular capability.

6. Claims 19 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Jamtgaard and Wilf, further in view of Laraki.

Regarding Claim 19,

Aura as modified by Jamtgaard and Wilf does not explicitly disclose providing the mobile device identifier based on at least one of a MIN, an ESN, and an application serial number.

Laraki, however, discloses providing the mobile device identifier based on at least one of a MIN, an ESN, and an application serial number (Paragraph 53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard and Wilf in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

Regarding Claim 23,

Aura as modified by Jamtgaard and Wilf discloses the client of claim 18, in addition, Aura discloses data in the form of at least one device signature (Column 5, line 58 to Column 6, line 13; and Column 7, line 42 to Column 8, line 23); but may not explicitly disclose that sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions comprising: modifying the request to include at least one of a subscription identifier associated with the mobile device and a gateway identifier; forwarding the modified request to the server; receiving data from the server; and forwarding the data to the mobile device.

Laraki, however, discloses that sending the request further comprises sending the request to a carrier gateway, wherein the carrier gateway is configured to perform actions comprising: modifying the request to include at least one of a subscription identifier associated with the mobile device and a gateway identifier; forwarding the modified request to the server; receiving data from the server; and forwarding the data to the mobile device (Paragraphs 33-37 and 46-48). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the mobile subscription services of Laraki into the mobile authentication system of Aura as modified by Jamtgaard and Wilf in order to efficiently provide mobile users with access to content based upon subscriptions and affiliations in which a user will not be charged

twice for content that was previously paid for, but could not be downloaded prior to expiration of the subscription and is downloaded after expiration, thus improving reliability of the system.

7. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aura in view of Jamtgaard and Wilf, further in view of Kindberg.

Aura as modified by Jamtgaard and Wilf does not explicitly disclose receiving a munged URL associated with at least one device signature.

Kindberg, however, discloses receiving a munged URL associated with at least one device signature (Paragraphs 39 and 43-50). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the capability-enabled URL of Kindberg into the mobile authentication system of Aura as modified by Jamtgaard and Wilf in order to provide a simple mechanism by which a client can prove authorized access to resources via use of a modified URL including a signature corresponding to a particular capability.

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Meyer (U.S. Patent 6,741,681) shows a simple telephone without Internet capabilities accessing an Internet server.

Butler (U.S. Patent Application Publication 2003/0167334) shows the content server itself determining device capabilities and delivering content based on such capabilities.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **JEFFREY D. POPHAM** whose telephone number is (571)272-7215. The examiner can normally be reached on **M-F 9:00-5:30**.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham  
Examiner  
Art Unit 2137

/Jeffrey D Popham/  
Examiner, Art Unit 2137

/Emmanuel L. Moise/  
Supervisory Patent Examiner, Art Unit 2137